1. **Objetivo de la seguridad activa** Proteger y evitar daños en sistemas informáticos.
2. **Encriptación de datos** Tipo de seguridad activa.
3. **Reconocimiento social** Motivación de autorrealización.
4. **Ataques difíciles de detectar** Ataques pasivos.
5. **Suplantación de identidad** Ataque activo.
6. **Daño en ataques activos** Permanente.
7. **Malware perjudica a:** Usuarios y sistemas.
8. **Método común para combatir malware** Eliminación tras la infección.
9. **Malware con puertas traseras** Troyanos.
10. **Vulnerabilidades explotadas por backdoors** Puertos abiertos y contraseñas débiles.
11. **Uso principal de troyanos** Robo de datos bancarios.
12. **Malware que redirige servidores DNS** DNS hijackers.
13. **Ataque con mayor anonimato** Distribuido.
14. **Beneficio de conocer etapas de ataques** Pensar como atacantes.
15. **Fases de un ataque informático** Reconocimiento, acceso, mantenimiento, ocultación.
16. **Contramedida de los sistemas IDS** Evitar acceso prolongado.
17. **Red zombi** Equipos controlados sin permiso.
18. **Malware que modifica el sistema operativo** Rootkits.
19. **Descarga de malware por ventanas emergentes** Drive-by download.
20. **Secuestro de personas como objetivo del malware** No.
21. **Motivaciones de atacantes (seguridad activa)** Dinero, ideología, compromiso, ego.
22. **Mejor medida contra ataques pasivos** Cifrado.
23. **Ataque activo que impide uso de recursos** Denegación de servicios (DoS).
24. **Atención en ataques activos** Interrumpir el ataque.
25. **Atención en ataques pasivos** Proteger información.
26. **Contramedida en fase 3 de un ataque** Detección de ping.
27. **Eliminación de archivos log** Fase 5 (ocultación).
28. **Uso de información de ataques pasivos** Ataques activos.
29. **Dificultad en detectar ataques pasivos** Sin alteraciones visibles.
30. **Acrónimo MICE** Money, Ideology, Compromise, Ego.
31. **Criptominado se basa en:** Redes zombi.
32. **Diferencia entre keyloggers y stealers** Keyloggers registran teclas; stealers roban datos.
33. **Malware instalado como troyano** Spyware.
34. **Malware que satura recursos replicándose** Gusanos.
35. **Objetivo de herramientas preventivas** Impedir instalación de malware.
36. **Propagación de gusanos** Prevenirla deshabilitando carpetas compartidas.
37. **Definición de seguridad activa** Previene y combate amenazas.
38. **Objetivos de ataques pasivos** Interceptar y analizar datos.
39. **Propósito de un ataque activo** Modificar sistemas.
40. **No usar redes públicas** Protege información sensible.
41. **Objetivos del malware** Robar datos y secuestrar equipos.
42. **Malware que causa mal funcionamiento** Virus.
43. **Única solución para rootkits** Reinstalar sistema operativo.
44. **Envío de mensajes en cadena** Usar copia oculta (CCO).
45. **Incrementar seguridad en redes P2P** No almacenar datos sensibles.
46. **Crear cuentas con privilegios administrativos** Mantener acceso.
47. **Ataques evitados con técnicas agresivas** Activos.
48. **Malware que roba información sensible** Spyware.
49. **Codificar información en transporte** Aumenta seguridad.
50. **Responder a correos spam** Confirma dirección activa.
51. **Malware que cambia configuración del navegador** Hijacking.
52. **Malware que provoca ataques DoS/DDoS** Gusanos.
53. **Uso de correos no habituales** Para sitios no confiables.
54. **Descarga de software de seguridad** Desde el sitio oficial.
55. **IDS vs IPS** IDS detecta; IPS previene.
56. **Protección contra malware en navegadores** Certificados HTTPS.
57. **Qué monitorea un HIDS** Datos del host.
58. **Qué monitorea un NIDS** Toda la red.
59. **Malware que altera configuración del sistema** Adware.
60. **Beneficio de la encriptación** Protección de datos.
61. **Firewall combinado con IDS** Actúa como IPS.
62. **Método de detección de IPS** Basado en firmas y anomalías.
63. **Principal amenaza en redes sociales** Falta de privacidad.
64. **Protección en almacenamiento USB** Evitar ejecución automática.
65. **Medida contra ataques DoS** Cortafuegos.
66. **Software usado por NIDS** SmoothSec.
67. **Protección de contraseñas** Usar combinaciones complejas.
68. **Detección basada en firmas** Identifica malware conocido.
69. **Medida común contra malware** Antivirus actualizado.
70. **Fase crítica de ataque activo** Mantenimiento.
71. **Uso de detección de protocolos** Para DoS/DDoS.
72. **Ataque basado en comportamiento anómalo** Intrusiones desconocidas.
73. **Protección contra spyware** Bloqueo de rastreadores.
74. **Método preventivo más efectivo** Actualizaciones del sistema.
75. **Malware asociado a criptominería** Cryptojackers.